(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 23 249 A 1**

(51) Int. Cl.[7]:
G 06 F 12/14
H 04 L 12/00

(21) Aktenzeichen: 100 23 249.3
(22) Anmeldetag: 12. 5. 2000
(43) Offenlegungstag: 22. 11. 2001

DE 100 23 249 A 1

(71) Anmelder:
Martens, Jürgen, 70771 Leinfelden-Echterdingen, DE

(74) Vertreter:
Schuster & Partner, 70174 Stuttgart

(72) Erfinder:
gleich Anmelder

(56) Entgegenhaltungen:
US 58 32 208

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Vermeidung von unkontrolliertem und/oder unberechtigtem Zugriff auf Computer im Wege von E-Mails

(57) Es wird ein Verfahren zur Erkennung und Bearbeitung von E-Mails vorgeschlagen, bei dem die E-Mail beim Server angefordert wird, anschließend E-Mail auf aktive Inhalte überprüft wird, dann die aktiven Inhalte der E-Mail deaktiviert werden und schließlich eine Benutzerinformation über die Veränderung der E-Mail erfolgt.

DE 100 23 249 A 1

Beschreibung

Stand der Technik

[0001] Zum Schutz von Computern gegen Verlust, Manipulation oder den unbemerkten Diebstahl von Daten durch unberechtigten Dateizugriff durch Dateien, die aktive Inhalte, wie z. B. Viren, Trojanische Pferde, Würmer, Makroviren, enthalten, die im Folgenden auch unter dem Sammelbegriff "Viren" zusammengefaßt werden, sind Gegenprogramme, sogenannte Virenscanner, entwickelt worden. Diese durchsuchen die Speichermedien (Festplatte, Diskettenlaufwerk) nach aktiven Inhalten und versuchen, (beispielsweise nach erfolgreicher Virusidentifizierung) die befallene Datei zu eliminieren. Da Viren eigenständige Befehlsfolgen oder Programme sind, und diese von den auf dem Speichermedium vorhandenen und erwünschten Programmen unterschieden werden müssen, werden alle auf dem Speichermedium vorhandene Dateien nach charakteristischen Befehlsfolgen bekannter Viren durchsucht. Neuere Virenscanner beziehen dabei auch Makros z. B. aus Textverarbeitungsprogrammen und sog. Skript-Dateien in ihre Untersuchung mit ein. Trotz des Einsatzes von Virenscannern kommt es immer dann zu Schadensfällen, wenn aktive Inhalte wegen ihres bisher unbekannten Befehlsmusters vom Virenscanner unerkannt bleiben.

[0002] Da ein häufiger Übertragungsweg für Viren der Empfang elektronischer Nachrichten, sog. eMails ist, werden Virenscanner auch eingesetzt, um auf das Speichermedium heruntergeladene Anhangsdateien von eMails zu untersuchen. Die eMail-Nachricht selbst, an die eine infizierte Datei angehängt ist, kann in der Regel geöffnet und gelesen werden, da das Mail-Programm wie ein Texteditor arbeitet und dieser im Normalfall den Inhalt nur anzeigt und nicht interpretiert. Eine eMail-Nachricht kann somit selbst kein Virus sein. Sie kann aber möglicherweise einen enthalten. So können beispielsweise unter gewissen Umständen, die durch falsch gewählte Sicherheitseinstellungen des Mail-Programms hervorgerufen werden können, Sicherheitslükken entstehen, die dann zusammen mit dem ausgewählten mailprogramm-spezifischen Automatismus den in HTML-Mails enthaltenen aktiven Inhalt nach dem Öffnen dieser eMail aktivieren.

Die Erfindung und ihre Vorteile

[0003] Das erfinderische Verfahren verhindert das Auftreten derartiger Schadensfälle, indem aktive Inhalte insbesondere einer eMail vor dem Öffnen der Datei bzw. Nachricht erkannt und unschädlich gemacht werden.

[0004] Das erfinderische Verfahren erreicht dieses Ziel auf folgende Weise:

[0005] Bei der eMail-Anforderung vom Server werden die eMails nach aktiven Inhalten überprüft. Hierbei ist es denkbar, daß die eMails aus dem Server im Internet in einen Zwischenspeicher geladen werden Dabei ist es notwendig, dem bisherigen einen neuen POP3-Client vorzuschalten.

[0006] Die aktiven Inhalte werden deaktiviert. Diese Deaktivierung kann durch Verschlüsselung, Markierung der aktiven Inhalte in der Datei oder Nachricht oder durch Aussortieren eintreffender infizierter eMails erfolgen. Hierbei werden zuerst die Datei-Endungen der Anhangsdateien überprüft. Sollten dabei z. B. "exe"-, "com"-, "bat"-, "vbs"- oder ähnliche Dateien ermittelt werden, werden diese je nach Sicherheitseinstellung aus der eMail entfernt oder abgetrennt, verändert und auf dem Speichermedium, in der Regel der Festplatte, gespeichert. Bei dieser Deaktivierung werden auch bereits bekannt Viren erfaßt. Eine Löschung oder Veränderung, (vorteilhafterweise reversibel) abgetrennter Dateien oder Dateibestandteilen, vorteilhafterweise in Form einer Komprimierung oder Verschlüsselung, dient dazu, ein ungewolltes Öffnen der Datei zu verhindern.

[0007] Bereits komprimiert eingehende Dateien werden ebenso untersucht und schädliche Dateien werden deaktiviert.

[0008] Jede Veränderung der ursprünglichen eMail wird dem Benutzer angezeigt (Informationsausgabe). Ihm wird insbesondere das vorläufige Abtrennen von schädlichen Anhangsdateien mitgeteilt und die Entscheidung überlassen, die Abtrennung zu löschen oder anzunehmen.

[0009] Außerdem können auch Skript-Dateien, insbesondere an sich sichere Java-Skripte aus der eMail entfernt werden, falls diese in ihrem HTML-Teil aktive Inhalte übertragen.

[0010] Der Benutzer kann Art und Umfang für die Überprüfung auf aktive Inhalte selber einstellen. Beispielsweise wird ihm die Wahlmöglichkeit zwischen Löschen oder Erhalt des abgetrennten Teil eingeräumt. Sollte das Sicherheitsniveau etwas geringerer gewählt worden sein, wird der Inhalt der Dateien, die Daten schädigen können, nur auf vorher bestimmte Befehle durchsucht. Dateien werden demnach nur dann entfernt, wenn sie bestimmte Befehle enthalten. Auch Makros können so entfernt werden.

[0011] In einem zusätzlichen Schritt ist gemäß dem erfinderischen Verfahren die Entschlüsselung verschlüsselter eMails bei vorheriger Eingabe des Benutzerpaßworts vorgesehen.

[0012] Ist dieser Teil abgeschlossen, werden die (modifizierten) Nachrichten an das eMail-Programm übermittelt.

[0013] Bei Anwendung des erfinderischen Verfahrens ist eine Änderung der Einstellungen im eMail-Programm nur für die Adresse des POP3-Servers nötig. Ausgehende eMails bleiben davon unberührt.

[0014] Als weitere Sicherheitseinrichtung werden nach dem erfinderischen Verfahren alle Verbindungen abgewiesen, die nicht vom lokalen Rechner oder lokalen Netzwerk hergestellt werden.

[0015] Die einzelnen Verfahrensschritte des erfinderischen Verfahrens werden nicht sichtbar, sondern laufen im Hintergrund ab und werden durch Meldungen nur im Falle des Einschreitens angezeigt.

[0016] Außerdem kann das erfinderische Verfahren auch in Verbindung mit News-Servern eingesetzt werden.

[0017] Weitere Vorteile und vorteilhafte Ausgestaltungen der Erfindung sind den Ansprüchen entnehmbar.

[0018] Alle in der Beschreibung und den nachfolgenden Ansprüchen dargestellten Merkmale können sowohl einzeln als auch in beliebiger Kombination miteinander erfindungswesentlich sein.

Patentansprüche

1. Verfahren zur Erkennung und Bearbeitung von eMails **gekennzeichnet durch** folgende Verfahrensschritte:
   - Anforderung der eMail beim Server
   - Überprüfung der eMail auf aktive Inhalte
   - Deaktivieren der aktiven Inhalte der eMail
   - Benutzerinformation über die Veränderung der eMail.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Deaktivierung der aktiven Inhalte diese aus der eMail entfernt werden und auf einem Speichermedium abgelegt werden.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die aktiven Inhalte vor dem Ablegen auf das

Speichermedium komprimiert werden.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zur Deaktivierung der aktiven Inhalte diese gelöscht werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß eine verschlüsselt eingegangene eMail vor ihrer Überprüfung entschlüsselt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß Verbindungen abgewiesen werden, die nicht vom lokalen Rechner oder dem lokalen Netzwerk hergestellt werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß eine Zwischenspeicherung der angeforderten eMail erfolgt.

- Leerseite -